CLAIMS

What is claimed is:

1. A system for authenticating a client device requesting a session of service from a service provider, comprising:

at least two matching one-time pad cryptological tables, a first of which is stored in a client device, and a second of which is accessible by a service security server, each table having multiple entries, each entry including a field for a indicator of previous use, said previous use indicator for each entry being initialized in an "unused" state, each row containing at least one pad value;

a code exchanger for receiving a pad value from said client device by said service security server upon request for initiation of a service session;

a code comparator for determining if said received pad value is marked as "used" or "unused" in said second table;

a service session grantor configured to grant said service request responsive to determination that said received pad value is unused, including changing said used indicator to a "used" state upon said grant of service; and

a client device reconfigurator adapted to challenge said user of said client device responsive to determining that said received pad value is marked as "used", and to replace said first and second tables with new, synchronized tables responsive to successful response by said user to said challenge.

2. The system as set forth in Claim 1 wherein:

said one-time pad cryptological tables further comprise a sequence index;

said code comparator is further configured to determine if said received pad is the next unused pad according to said sequence indicators;

said session grantor is configured to grant a session only if said received pad is a next expected pad; and

said client device reconfigurator is adapted to respond to said received pad not being a next expected pad.

3. The system as set forth in Claim 1 wherein said code exchanger comprises at least one communications network selected from the group of a telephone network, a wireless data network, a Local Area Network, a Wide Area Network, and an Internet.

4. The system as set forth Claim 1 wherein client device reconfigurator is adapted to challenge said user with one or more methods selected from the group of requiring a user name input, requiring a password input, requiring an account number input, requiring an answer to a secret question, and requiring a user-designated response.

5. The system as set forth in Claim 1 wherein:

said one-time pad cryptological tables further comprise an expiration field for each entry;

said code comparator is further configured to determine if said received pad is expired;

said session grantor is configured to grant a session only if said received pad is unexpired; and

said client device reconfigurator is adapted to respond to said received pad being expired.

6. The system as set forth in Claim 1 wherein said client device reconfigurator is adapted to replace said tables using a secure replacement method.

7. The system as set forth in Claim 1 wherein said service session grantor is further configured to require a second step of acknowledgment between said service security server and said client device before said entry is marked as "used".

8. A method for authenticating a client device requesting a session of service from a service provider, said method comprising the steps of:

providing at least two matching one-time pad cryptological tables, disposing a first of which in a client device, and disposing a second of which such that it is accessible by a service security server, each table having multiple entries, each entry including a field for an indicator of previous use, said previous use indicator for each entry being initialized in an "unused" state, each row containing at least one pad value;

receiving a pad value from said client device by said service security server upon request for initiation of a service session;

determining if said received pad value is marked as "used" or "unused" in said second table;

responsive to determination that said received pad value is unused, granting said service request and changing said used indicator corresponding to said pad entry in said second table to a "used" state; and

responsive to determining that said received pad value is marked as "used", challenging said user of said client device, and replacing said first and second tables with new, synchronized tables responsive to successful response by said user to said challenge.

9. The method as set forth in Claim 8 wherein:

said step of providing one-time pad cryptological tables further comprises providing a sequence index field for each table entry;

said step of determining if said received pad is used comprises determining if said received pad is the next unused pad according to said sequence indicators;

said step of granting a session comprises granting a session only if said received pad is a next expected pad; and

said step of challenging said user comprises challenging said user responsive to said received pad not being a next expected pad.

10. The method as set forth in Claim 8 wherein said step of receiving a pad value comprises receiving a pad value via at least one communications network selected from the group of a telephone network, a wireless data network, a Local Area Network, a Wide Area Network, and an Internet.

11. The method as set forth in Claim 8 wherein said step of challenging a user comprises challenging a user with one or more methods selected from the group of requiring a user name input, requiring a password input, requiring an account

number input, requiring an answer to a secret question, and requiring a user-designated response.

12. The method as set forth in Claim 8 wherein:

said step of providing one-time pad cryptological tables further comprises providing an expiration field for each entry;

said step of determining if said received pad comprises determining if said received pad is expired;

said step of granting a session comprises granting a session only if said received pad is unexpired; and

said step of challenging a user and replacing said tables comprises challenging a user if said received pad is determined to be expired.

13. The method as set forth in Claim 8 wherein said step of replacing said tables comprises using a secure replacement method to provide said replacement table to said client device.

14. The method as set forth in Claim 8 wherein said step of granting a service session comprises a second step of acknowledgment between said service security server and said client device before said entry is marked as "used".

15. A computer readable medium encoded with software for authenticating a client device requesting a session of service from a service provider, said software performing the steps of:

providing at least two matching one-time pad cryptological tables, disposing a first of which in a client device, and disposing a second of which such that it is accessible by a service security server, each table having multiple entries, each entry including a field for an indicator of previous use, said previous use indicator for each entry being initialized in an "unused" state, each row containing at least one pad value;

receiving a pad value from said client device by said service security server upon request for initiation of a service session;

determining if said received pad value is marked as "used" or "unused" in said second table;

responsive to determination that said received pad value is unused, granting said service request and changing said used indicator corresponding to said pad entry in said second table to a "used" state; and

responsive to determining that said received pad value is marked as "used", challenging said user of said client device, and replacing said first and second tables with new, synchronized tables responsive to successful response by said user to said challenge.

16. The computer readable medium as set forth in Claim 15 wherein:

said software for providing one-time pad cryptological tables further comprises software for providing a sequence index field for each table entry;

said software for determining if said received pad is used comprises software for determining if said received pad is the next unused pad according to said sequence indicators;

said software for granting a session comprises software for granting a session only if said received pad is a next expected pad; and

said software for challenging said user comprises software for challenging said user responsive to said received pad not being a next expected pad.

17. The computer readable medium as set forth in Claim 15 wherein said software for receiving a pad value comprises software for receiving a pad value via at least one communications network selected from the group of a telephone network, a wireless data network, a Local Area Network, a Wide Area Network, and an Internet.

18. The computer readable medium as set forth in Claim 15 wherein said software for challenging a user comprises software for challenging a user with one or more

methods selected from the group of requiring a user name input, requiring a password input, requiring an account number input, requiring an answer to a secret question, and requiring a user-designated response.

19. The computer readable medium as set forth in Claim 15 wherein:

said software for providing one-time pad cryptological tables further comprises software for providing an expiration field for each entry;

said software for determining if said received pad comprises software for determining if said received pad is expired;

said software for granting a session comprises software for granting a session only if said received pad is unexpired; and

said software for challenging a user and replacing said tables comprises software for challenging a user if said received pad is determined to be expired.

20. The computer readable medium as set forth in Claim 15 wherein said software for replacing said tables comprises software for using a secure replacement method to provide said replacement table to said client device.

21. The computer readable medium as set forth in Claim 15 wherein said software for granting a service session comprises software for performing a second step of

acknowledgment between said service security server and said client device before said entry is marked as "used".